EXERCICE 26 : cryptographie, le chiffrement de Hill

Notation : soit $A=(a_{ij})$ et $B=(b_{ij})$ deux matrices d'entiers de même dimension ; on écrira $A \equiv B$ [mod 26] pour signifier que $a_{ij} \equiv b_{ij}$ [mod 26] pour tous i et j. .

Nous admettrons la propriété suivante : si $A \equiv B$ [mod 26] et si C est une matrice d'entiers telle que les produits matriciels AC et BC existent, alors $AC \equiv BC$ [mod 26]. De même, si D est une matrice d'entiers telle que les produits matriciels DA et DB existent, alors $DA \equiv DB$ [mod 26].

Principe du chiffrement de Hill :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Nombre	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pour coder un mot de deux lettres, on remplace chaque lettre du mot par un entier en utilisant le tableau ci-dessus ; on associe à ce mot une matrice colonne X à deux lignes, la première ligne contenant l'entier correspondant à la première lettre du mot et la deuxième ligne contenant l'entier correspondant à la deuxième lettre du mot. On se donne une matrice A carrée d'ordre 2 appelée matrice de chiffrement. On calcule le produit matriciel AX puis on détermine la matrice colonne Y à deux lignes dont tous les coefficients sont des entiers compris entre 0 et 25 et qui vérifie $AX \equiv Y$ [mod 26]. Cette matrice Y permet de construire, grâce au tableau ci-dessus, un mot de deux lettres qui code le mot de départ.

Pour coder un mot de plus de deux lettres, on le découpe en blocs de deux lettres et on applique la méthode ci-dessus à chaque bloc.

1) Cryptage.

a) On considère la matrice de chiffrement $A_1 = \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$. Coder le mot HILL.

b) On considère la matrice de chiffrement $A_2 = \begin{pmatrix} 4 & 2 \\ 3 & 8 \end{pmatrix}$. Coder le mot AMER.

Quel est le problème posé par cette matrice A_2 ?

2) Réversibilité du cryptage.

Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On pose $\delta = ad - bc$.

Soit deux matrices $X = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ et $X' = \begin{pmatrix} x'_1 \\ x'_2 \end{pmatrix}$, formées d'entiers compris entre 0 et 25, telles que $AX \equiv AX'$ [mod 26].

a) Calculer les produits matriciels AX et AX'.

b) Montrer que $\delta(x_1 - x'_1) \equiv 0$ [mod 26] et que $\delta(x_2 - x'_2) \equiv 0$ [mod 26].

c) Démontrer que si δ et 26 sont premiers entre eux, alors $X = X'$.

d) Montrer que δ et 26 sont premiers entre eux dans le cas de la matrice A_1 mais pas dans le cas de A_2.

3) Décryptage.

Dans cette partie on prend $A = \begin{pmatrix} 2 & 5 \\ 3 & 4 \end{pmatrix}$.

Sachant que $AX \equiv Y$ [mod 26] on va chercher une matrice B telle que $X \equiv BY$ [mod 26].

a) Montrer que la matrice A est inversible et déterminer A^{-1}.

Pourquoi cette matrice A^{-1} ne peut-elle pas être la matrice B recherchée pour le décryptage ?

b) Soit $C = \begin{pmatrix} -4 & 5 \\ 3 & -2 \end{pmatrix}$. Montrer que $CA = 7I_2$.

c) Déterminer un entier u compris entre 0 et 25 tel que $7u \equiv 1$ [mod 26].

d) Soit B la matrice carrée d'ordre 2 formée d'entiers compris entre 0 et 25 telle que $B \equiv uC$ [mod 26]. Montrer que $BA \equiv I_2$ [mod 26].

e) En déduire que $X \equiv BY$ [mod 26]

f) Calculer les coefficients de la matrice B et décoder le mot MATH.